UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

MARIA RUSKIEWICZ, et al.	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 5:23-cv-00303-D**
	)	
OKLAHOMA CITY UNIVERSITY,	)	
	)	
Defendant.	)	

REPLY BRIEF IN SUPPORT OF DEFENDANT'S
MOTION TO DISMISS THE CLASS ACTION COMPLAINT

Plaintiff has failed to demonstrate she has a concrete and particularized injury caused by Oklahoma City University ("OCU") and which is redressable by this Court so as to give her Article III standing. Her response articulates four—and only four—categories of alleged harm that she argues should give her standing. (Doc. 30, pp. 7-11.) However, her allegations are identical to those already considered and rejected by this Court in *Legg v. Leaders Life Insurance* Company, 574 F.Supp.3d 985 (W.D. Okla. 2021), and none of them constitute a concrete and particularized injury. Therefore, the same conclusion should be reached in this case and Plaintiff's complaint should be dismissed.[1]

A. Plaintiff's Characterization of the Facts Requires Clarification

In support of her arguments that she has standing, Plaintiff makes certain factual assertions in her response that are inaccurate and require clarification.

[1] Even if Plaintiff has standing, each of her causes of action fails to state a claim upon which relief can be granted for the reasons already advanced in OCU's opening brief. For purposes of this reply, however, OCU rests on the arguments in its opening brief as to those issues and only addresses the issue of standing.

First, Plaintiff states that OCU made a "disclosure" of her information and "publicized" it "to enough people that it is reasonably likely those facts have and/or will become known to the public at large[.]" (Doc. 30, p. 8.) But to clarify, OCU did not "disclose" any information to the cybercriminals, nor did it "publicize" anything to anyone, let alone "the public at large." Rather, OCU was the victim of a ransomware attack in which cybercriminals encrypted its network and, in the process, took certain files without OCU's authorization or knowledge. Thus, any disclosure or publication of Plaintiff's information was made by the cybercriminals, not by OCU.

Second, implicitly acknowledging that the cybercriminals, not OCU, are responsible for any disclosure or publication of her information, Plaintiff states that "criminals frequently post stolen private information openly and directly on various 'dark web' internet websites, making the information publicly available, for a substantial fee, of course." (Doc. 30, p. 8.) Even if that is true in some cases, Plaintiff does not allege that occurred with respect to her data. In addition, a cybercriminal posting something on the dark web is far different than posting it on the world wide web or publicizing it "to the public at large." The dark web is not readily accessible or navigable, as it consists of hidden sites that cannot be found through conventional web browsers.[2] These hidden sites are not indexed on search engines. *Id.* As such, to navigate the dark web, one must obtain access through certain networks created specifically for the dark web.[3]

[2] NortonLifeLock, *What is the dark web and how do you access it?* https://us.norton.com/blog/how-to/how-can-i-access-the-deep-web (visited Aug. 28, 2023)
[3] Wikipedia, *Dark web*, https://en.wikipedia.org/wiki/Dark_web (visited Aug. 28, 2023).

Third, Plaintiff still fails to allege any actual or attempted misuse of her information that was supposedly disclosed or publicized by the cybercriminals. Indeed, courts have recognized that the purpose of ransomware attacks like those on OCU "is the exchange of money for access to data, not identity theft." *In re Practicefirst Data Breach Litigation*, No. 1:21-CV-00790(JLS/MJR), 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022). And even if someone wanted to do something malicious with the files the cybercriminals took from OCU, there remains a "speculative chain of possibilities" that would first have to occur before causing harm to Plaintiff, including locating the data on the dark web, successfully purchasing or downloading it, identifying Plaintiff's information within the documents, and then successfully misusing the information without getting caught and without any procedural safeguards preventing it (e.g. credit monitoring, account verification, etc.), none of which Plaintiff alleges happened in this case. *See Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 410 (2013) (no standing where theory rested on "highly attenuated chain of possibilities").

B. Plaintiff Remains Unable to Plausibly Allege a Concrete, Particularized, and Actual or Imminent Injury Sufficient to Establish Article III Standing.

Plaintiff's response articulates four—and only four—categories of alleged harm that she argues should give her standing. (Doc. 30, pp. 7-11.) However, none of these theories have any merit, and OCU addresses each in turn below.

1. Plaintiff's Allegations Are Not Analogous to a Traditionally Recognized Harm That Provides a Basis for a Lawsuit

Plaintiff first argues that "the disclosure of Personal Information itself in the Data Breach is analogous to traditionally recognized harm of disclosure of private information

to confer standing." (Doc. 30, p. 8.) In support, she cites to *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), in which the Supreme Court stated that part of assessing concreteness is "whether the asserted harm has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 2200. In *TransUnion*, the defendant credit reporting agency gave various third parties credit reports which labeled the plaintiffs as "potential terrorists, drug traffickers, or serious criminals." *Id.* at 2209. As such, the Supreme Court found they suffered a concrete harm with a close relationship to the traditionally recognized tort of defamation. *Id.*

Here, Plaintiff tries to analogize that she has suffered harm with a close relationship to the traditionally recognized tort of disclosure of private information. But this analogy fails because, as discussed above, OCU did not disclose or publicize anything about Plaintiff. Rather, any such disclosure or publication was by the cybercriminals after they took the files from OCU. *See, e.g. In re Ambry Genetics Data Breach Litig.*, No. SACV2000791CJCKESX, 2021 WL 4891610, at *9 (C.D. Cal. Oct. 18, 2021) (dismissing claim in proposed data breach class action under California's Confidentiality of Medical Information Act barring unauthorized "disclosure" of protected health information, noting that: "'Disclose' is an active verb, denoting … an affirmative act of communication" and finding the plaintiffs "do not allege that Defendants performed any affirmative communicative act that gave hackers information.").

In that regard, *TransUnion* recognized there is no historical or common-law analog where an element "essential to liability" is missing. *Id.* at 2209-10. And for a defendant to be liable for the tort of public disclosure of private information, it must have "publicized"

the information about the plaintiff, which requires that "the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge[.]" *Eddy v. Brown*, 715 P.2d 74, 78 (1986).[4] Similarly, Black's Law Dictionary defines "publication" as "the act of declaring or announcing to the public." PUBLICATION, Black's Law Dictionary (11th ed. 2019). Yet in this case, it simply is not and cannot plausibly be alleged that OCU committed any act of publication to announce, communicate, or declare to the public any of Plaintiff's private information.

Again, this matter arises out of a ransomware attack in which cybercriminals took files from OCU's computer network without its authorization or knowledge. OCU obviously did not give Plaintiffs information to the cybercriminals. It did not publish Plaintiff's information on the dark web. And it certainly did not announce or communicate Plaintiff's information to the public at large. Rather, any publication of Plaintiff's information occurred solely at the hands of the cybercriminals after they took the files from OCU. Thus, Plaintiff's reliance on *TransUnion* is misplaced, and she has not suffered a harm that gives her standing. *See also Aponte v. Northeast Radiology, P.C.*, No. 21 CV

[4] The comments to Restatement 2d of Torts § 625D provide, "The form of invasion of the right of privacy covered in this Section depends upon publicity given to the private life of the individual. 'Publicity,' as it is used in this Section, differs from 'publication,' as that term is used in § 577 in connection with liability for defamation. 'Publication,' in that sense, is a word of art, which includes any communication by the defendant to a third person. 'Publicity,' on the other hand, means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge. The difference is not one of the means of communication, which may be oral, written or by any other means. It is one of a communication that reaches, or is sure to reach, the public."

5883 (VB), 2022 WL 1556043 at *5 (S.D.N.Y. May 16, 2022) (where unauthorized third parties, not defendants, improperly accessed plaintiffs' data, "plaintiffs have not identified a close historical or common-law analogue to the alleged injuries they suffered from defendants' actions."); *In re Practicefirst*, 2022 WL 354544 at *7 (no common law analogue where data not disclosed to public at large).

2. Plaintiff Remains Unable to Manufacture Standing

Plaintiff next argues that she and the class have standing because they allegedly "have been required to take measures to deter and detect identity theft and fraud, such as placing 'freezes' and 'alerts' with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts and closely reviewing and monitoring their credit reports, and accounts for unauthorized activity." (Doc. 30 at 15.) She also argues they "have suffered costs associated with this lost time and effort to mitigate the consequences of the Data Breach, and will be forced to do so into the future." (*Id.*)

In support, Plaintiff relies on an unpublished Sixth Circuit decision, *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016), and a district court case from that circuit applying *Galaria*, which found allegations of corrective measures and lost time and expense sufficient for standing. However, this Court already examined and distinguished *Galaria*, noting that "the complaint in *Galaria* included an allegation that the named class representative had already been the victim of attempted fraud." *Legg*, 574 F.Supp.3d at 990. Here, there is no allegation that Plaintiff already has been the victim of attempted fraud or suffered any misuse of her data. Accordingly, *Galaria* is inapplicable.

Yet even if *Galaria* had similar facts, its reasoning is incorrect and should not be followed because it contradicts *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 402 (2013), which held that plaintiffs "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending." Indeed, this Court correctly applied *Clapper* to reject this same argument in *Legg*. When the plaintiff in *Legg* argued that he "suffered an 'actual injury' in the form of lost time, money, and annoyance associated with responding to the data breach," this Court cited *Clapper* and correctly stated that "a plaintiff cannot 'manufacture standing' simply by incurring certain costs as a reasonable reaction to a risk of harm." *Legg*, 574 F. Supp. 3d at 994.

The same is true here. Even if Plaintiff alleged facts that she took steps to mitigate potential harm (which she does not do), those actions cannot be used to manufacture standing for this case. *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344-45 (11th Cir. 2021) ("Tsao cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft"); *In re SuperValu, Inc.*, 870 F.3d 763, 769 (8th Cir. 2017) ("the time they spent protecting themselves against this speculative threat cannot create an injury"); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011) ("Appellants' alleged time and money expenditures to monitor their financial information do not establish standing").

3. Plaintiff Does Not Plausibly Allege an Actual, Present Emotional Injury

Plaintiff's third argument is that she "has suffered currently felt harms of embarrassment, humiliation, frustration, and emotional distress by the Data Breach." (Doc. 30, p. 16.) She premises this on *dicta* in *TransUnion* in which the Supreme Court noted

that the plaintiffs did not present evidence they were "independently harmed by their exposure to the risk itself—that is, they suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses." *Id.* However, the Supreme Court made clear this was merely hypothetical and cautioned that "[w]e take no position on whether or how such an emotional or psychological harm could suffice for Article III purposes—for example, by analogy to the tort of intentional infliction of emotional distress." *TransUnion*, 141 S. Ct. at 2211, n. 7. Thus, it should not be read as creating license for potential plaintiffs to conjure standing in data breach cases merely by uttering the words "emotional harm."

Indeed, the plaintiffs in *Legg* also alleged that the "threat of fraud and identity theft" caused them "increased emotional distress and anxiety." *Legg*, 574 F. Supp. 3d at 988. However, there remained no allegations of misuse of the plaintiffs' information or any other form of harm, and the Court held they lacked standing. *Id.* at 994-995. The absence of such allegations thus distinguishes *Legg* and this case from the other case cited by Plaintiff in her response, *Bowen v. Paxton Media Grp., LLC*, No. 5:21-CV-00143-GNS, 2022 WL 4110319 (W.D. Ky. Sept. 8, 2022), in which the plaintiffs alleged emotional distress as a form of damages, but not in isolation, but rather in connection with several instances of actual misuse of their information, including fraudulent loans, identity theft, and the opening of a fraudulent bank account. *Id.* at *4. In contrast, Plaintiff does not allege any such misuse of her information.

Other courts also have rejected the notion that a data breach plaintiff can establish standing merely by claiming to have experienced emotional distress, noting that, if that

were true, the entire doctrine of standing would turn into a farce. For instance, one court held that allegations of "mental aggravation, anxiety, and emotional distress from the data breach" remain insufficient to provide standing because "such emotional injuries constitute quintessential abstract harms that are beyond the Court's power to remedy." *Kim v. McDonald's USA, LLC*, No. 21-CV-05287, 2022 WL 4482826, at *6 (N.D. Ill. Sept. 27, 2022). Noting the potential slippery slope, the court further said, "if these emotional injuries alone were sufficient to invoke the jurisdiction of federal courts, then everyone would have standing to litigate about everything." *Id. See also In re Illuminate Educ. Data Sec. Incident Litig.*, No. SACV221164JVSADSX, 2023 WL 3158954, at *4 (C.D. Cal. Apr. 19, 2023) (plaintiffs lacked standing based on alleged emotional distress from data breach); *Wadsworth v. Kross, Lieberman & Stone, Inc.*, 12 F.4th 665, 668 (7th Cir. 2021) (emotional harm not insufficient to confer standing).

Plaintiff also does not even plausibly allege emotional harm from the data breach. It is telling that, in her complaint, Plaintiff identified several categories of alleged damages that she and the class "have suffered or are at increased risk of suffering," yet that list did not include any alleged emotional injury. (Doc. 1, ¶ 72.) In her response, Plaintiff cites paragraph 99 of the complaint, which appears to be the sole reference to any alleged emotional injury and which merely states, "Plaintiff and Members of the Class ***have suffered or will suffer injury*** and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress." *Id.* (Emphasis added.) This isolated and boilerplate reference is wholly insufficient to allege a plausible claim for emotional harm, particularly when

viewed in the absence of any misuse of Plaintiff's information or any other actual harm. *See also Coddington v. Crow*, No. 22-6100, 2022 WL 10860283, at *9 (10th Cir. Oct. 19, 2022) ("if current emotional distress based on fear of future harm is enough for injury-in-fact, we believe that such a fear would need to be reasonably founded")

4. Plaintiff Remains Unable to Plausibly Allege an Actual, Present Injury Based on Diminished Value of Her Personal Information.

Finally, Plaintiff argues she has suffered a concrete injury because her personal information allegedly has diminished value to herself and on the black market. (Doc. 30, pp.16-17.) In support, she cites cases regarding diminished value of personal information, mostly from the Ninth Circuit, which are not binding on this Court. However, this Court already addressed and correctly rejected the diminished value argument. *See Legg*, 574 F. Supp. 3d at 994. Without factual allegations showing that Plaintiff tried to sell her personal information and was forced to accept a lower price because the information was already available through the data breach, this allegation amounts to nothing more than a hypothetical and conjectural injury. *See also In re Practicefirst*, 2022 WL 354544, at *5 (no standing based on diminished value where no allegations of attempted sale).

Signature on following page

Respectfully submitted, this 1st day of September, 2023.

/s/ David A. Cole
David A. Cole
Georgia Bar No. 142383
FREEMAN MATHIS & GARY, LLP
100 Galleria Parkway, Suite 1600
Atlanta, GA 30339
(770) 818-0000
Admitted pro hac vice

Timothy B. Soefje
Oklahoma Bar No. 33342
Kai Hecker
Texas Bar No. 24028463
FREEMAN MATHIS & GARY, LLP
5851 Legacy Circle, 6th Floor
Plano, TX 75024
(469) 895-3005

Teddy Abbot
COOK & HILFIGER, P.C.
620 West Broadway
Muskcogee, OK 74401
teddy@cookhilfiger.com

Attorneys for the Defendant
Oklahoma City University